Civilian Research Project
USAWC Fellow

NATO's Options for Defensive Cyber Against Non-State Actors

by

Colonel Casimir C. Carey III
United States Army

United States Army War College
Class of 2013

REPORT DOCUMENTATION PAGE	Form Approved OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
xx-04-2013	CIVILIAN RESEARCH PROJECT	

4. TITLE AND SUBTITLE
NATO's Options for Defensive Cyber Against Non-State Actors

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Colonel Casimir C. Carey III
United States Army

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Professor William C. Banks
Syracuse University

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Ms. Karen J. Finkenbinder

U.S. Army War College, 122 Forbes Avenue, Carlisle, PA 17013

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution A: Approved for Public Release. Distribution is Unlimited.

13. SUPPLEMENTARY NOTES
Word Count: 5,965

14. ABSTRACT

Overt state-to-state cyber conflicts are unlikely for the foreseeable future; states prefer to retain plausible deniability through surreptitious sponsorship of non-state cyber militias. International legal norms, NATO's Article 5 requirements, and UN Security Council procedural issues seem to limit NATO's options in responding to cyber events by non-state actors. However, there are three circumstances under which NATO may legally take cyber countermeasures against non-state actors: (1) when a nation-state fails to enforce the law against non-state actors within its borders; (2) when a cyber-disruption is tantamount to an economic blockade; and (3) if there is intelligence that indicates a pending cyber-attack by force, thereby necessitating anticipatory self-defense. The decision by NATO after 9/11 to pursue a non-state terrorist organization was a normative shift internationally; prior to this event, counterterrorism was widely viewed as a law enforcement issue. With China and Russia as permanent members of the UN Security Council, resolutions against countries for harboring cyber militias are unlikely. Both nations routinely tolerate—if not sponsor—cyber militias. NATO is the one enforcement arm with the resources to thwart the illicit militias.

15. SUBJECT TERMS
Anticipatory Self-Defense, blockade, DDOS, Tallinn Manual, Article 5, Estonia, rule of law, countermeasures

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			19b. TELEPHONE NUMBER *(Include area code)*
UU	UU	UU	UU	36	

USAWC CIVILIAN RESEARCH PROJECT

NATO's Options for Defensive Cyber Against Non-State Actors

by

Colonel Casimir C. Carey III
United States Army

Professor William C. Banks
Syracuse University
Project Adviser

Ms. Karen J. Finkenbinder
U.S. Army War College Faculty Mentor

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

Abstract

Title:	NATO's Options for Defensive Cyber Against Non-State Actors
Report Date:	April 2013
Page Count:	36
Word Count:	5,965
Key Terms:	Anticipatory Self-Defense, blockade, DDOS, Tallinn Manual, Article 5, Estonia, rule of law, countermeasures
Classification:	Unclassified

Overt state-to-state cyber conflicts are unlikely for the foreseeable future; states prefer to retain plausible deniability through surreptitious sponsorship of non-state cyber militias. International legal norms, NATO's Article 5 requirements, and UN Security Council procedural issues seem to limit NATO's options in responding to cyber events by non-state actors. However, there are three circumstances under which NATO may legally take cyber countermeasures against non-state actors: (1) when a nation-state fails to enforce the law against non-state actors within its borders; (2) when a cyber-disruption is tantamount to an economic blockade; and (3) if there is intelligence that indicates a pending cyber-attack by force, thereby necessitating anticipatory self-defense. The decision by NATO after 9/11 to pursue a non-state terrorist organization was a normative shift internationally; prior to this event, counterterrorism was widely viewed as a law enforcement issue. With China and Russia as permanent members of the UN Security Council, resolutions against countries for harboring cyber militias are unlikely. Both nations routinely tolerate—if not sponsor—cyber militias. NATO is the one enforcement arm with the resources to thwart the illicit militias.

NATO's Options for Defensive Cyber Against Non-State Actors

Estonia's Minister of Defence—Jaak Aaviksoo—noted with alarm a massive increase in Internet queries directed against the tiny Baltic state's government and commercial web servers in early May 2007. Suspecting the hand of Russia in this expanding Distributed Denial of Service (DDOS) attack, he urgently requested assistance from the North Atlantic Treaty Organization (NATO)—of which Estonia had been a member since 2004. To his frustration, he vented to international media that "NATO does not define cyber-attacks as a clear military action. This means that…collective self defence, will not automatically be extended to the attacked country."[1] Aaviksoo's suspicions about Kremlin sponsorship were understandable, given the ongoing dispute between native Estonians and ethnic Russian citizens—in response to the government's decision to reposition the "Bronze Soldier" war memorial statue from downtown Tallinn to a suburban military cemetery. The government's intent was to stop the annual conflicts that routinely occurred during the 9 May "Victory Day" observance of the Soviet Union's triumph over Nazi Germany. Ethnic Russians typically spent the day honoring their war dead; native Estonians viewed the occasion as an unpleasant reminder of Soviet occupation from 1944-1991, and sardonically referred to the Bronze Soldier as "the Unknown Rapist."[2] The statue's displacement proved to be a tipping point that touched off riots and looting by thousands of ethnic Russian Estonians—leaving 800 arrested, 153 injured, and one dead.[3] Ethnic Russians throughout Eurasia took umbrage to the perceived insult to veterans and survivors of the "Great Patriotic War," which generated conspiratorial activity on the Russian-language Internet forums—urging followers to disable Estonia's Internet infrastructure.[4] The cyber event began with "Script-kiddies"—amateurish cyber activists who copy

programs from hacker websites—initiating demands on Estonian websites with simple "ping" attacks.[5] Two weeks later—just hours before "Victory Day" itself—Estonian government, banking, and business websites received a 200-fold increase in traffic from nearly a million unwittingly enslaved "botnet" computers worldwide.[6] A "bot" is a computer infected by malware that reprograms it to respond to an external server—often in a different country.[7] It was through these botnets that demands for bandwidth increased exponentially—from 1,000 packets[8] per day on 26 April to 2,000 packets per hour on 27 April to *4 million packets per second* on 9 May 2007. Hundreds of targeted websites crashed from an inability to handle the volume of packets directed to them.[9] Neither the European Union nor NATO could find evidence of direct collusion between the Russian government and the hackers who fomented the DDOS against Estonian governance and commerce,[10] but lost revenue and information technology expenses to Estonian businesses amounted to an estimated 3 million euros.[11] Estonia lost over 1.85% of its 2007 GDP; an incident on the same scale in the United States would cost US citizens nearly $260 billion,[12] which is comparable to the entire Gross State Product of Arizona in 2007;[13] at the time, Arizona had the United States' nineteenth-largest state economy.[14] From Estonia's perspective, the crippling effect of the DDOS on its heavily Internet-dependent country warranted action by NATO. The argument for *jus a bellum*—"right to war"—is fairly clear in state-to-state conflicts, but in this case ostensibly non-state actors were responsible for disrupting a sovereign nation-state to the extent of crippling its economy. The North Atlantic Treaty's Article 5 was intended to rally Western European countries against a Warsaw Pact border incursion during the Cold War; yet since NATO's formation in 1949, the alliance has invoked Article 5 just

once—after the 9/11 attacks upon the United States in 2001. Article 5 addresses collective self-defense, to which NATO's twenty-eight signatories agree that "an armed attack against one or more of them in Europe or North America shall be considered an attack against them all."[15] Lord Robertson—NATO's Secretary General during Al Qaeda's attacks against the World Trade Center and the Pentagon—stated that the alliance invoked Article 5 at the time because "the attack against the United States on 11 September was directed from abroad and shall therefore be regarded as an action covered by Article 5 of the Washington Treaty."[16] Al Qaeda's status as a non-state actor evidently was not an impediment to mobilizing assistance for the United States. Yet in the case of Estonia, aside from providing some technical expertise and holding discussions among the NATO ministers, the alliance offered no response—despite highly sophisticated cyber capabilities in the United States, the United Kingdom, and France that easily could have dismantled botnets that relentlessly queried Estonian websites. Since the DDOS event did not cause physical damage or actual injury to Estonian citizens, NATO perceived itself lacking justification under international norms to respond with cyber in self-defense; unleashing cyber weapons to fend off attacks from the non-state cyber militia members would doubtlessly have been construed as an offensive action and breach of Russia's sovereignty at the time.

Under international norms, it is unlawful for NATO nations to conduct offensive cyber operations; except by means of an authorizing UN Security Council resolution, cyber actions must be under the rubric of self-defense. NATO's Cooperative Cyber Defence Centre of Excellence (CCD-CoE) recently published the *Tallinn Manual on the International Law Applicable to Cyber Warfare*, a three-year project by an "International

Group of Experts" in cyber technology and law. These experts determined that only "in the event that the use of force reaches the threshold of an armed attack is a state entitled to respond in self-defence"[17] with a cyber-attack by force. This is the crux of the problem for NATO's cyber defense activities: cyber events rarely rise to the level of armed attacks by nation-states. To further complicate matters, malware is unlikely to surface with "Made in Russia" written into its code; sponsoring nation-states prefer to maintain plausible deniability, rather than face the condemnation of the international community with revelations of compelling evidence verifying cyber misconduct. Non-state actors will be the likely users of malware for the foreseeable future, although the cyber weapons they employ may very well be provided through surreptitious state sponsorship.

Before the events of 9/11, nations saw attacks by non-state actors as a law enforcement issue. There was a normative shift, though, when the UN Security Council enacted increasingly restrictive sanctions on financial transactions, travel, and arms transfers intended by the international terrorist group Al Qaeda—regardless of its status as a non-state actor. One could extrapolate that cyber militias—almost always non-state actors—could be handled by the international community much like Al Qaeda, which still receives attacks by force nearly every week from NATO strikes. Unlike the physically violent actions associated with Al Qaeda, patriotic hacktivist groups sponsor cyber incidents with dubious characteristics as armed attacks—which puts NATO in a difficult legal position. Under current norms, using cyber countermeasures against non-state actors would violate the sovereignty of the states harboring them—even if they feign ignorance of cyber militias within their borders. The UN Charter's Articles 39 and

42 do, however, authorize the UN Security Council's use of force in response to "any threat to the peace…or act of aggression, and shall make recommendations" to employ "air, sea, or land forces as may be necessary to maintain or restore international peace and security."[18] Ideally, a UN Security Council resolution would pass—as it did in the case of Al Qaeda after 9/11—empowering NATO to shut down non-state cyber militias that disrupt or attack nation-states.

Five of the most advanced nations in cyber operations maintain permanent seats on the UN Security Council—the United States, Great Britain, France, Russia, and China; all five have veto power over a potential resolution. Russia and China run intrusive international cyber operations on a daily basis, as described by Director of National Intelligence James Clapper in his 31 January 2012 statement to the Senate Select Committee on Intelligence: "Among state actors, China and Russia are of particular concern…entities within these countries are responsible for extensive illicit intrusions into US computer networks and theft of US intellectual property."[19] Given China and Russia's apparent disregard for cyber sovereignty, it is unlikely that NATO would get any authority to pursue cyber defensive measures from the UN Security Council. In September 2012 China and Russia sponsored a draft cyber resolution at the UN General Assembly; NATO countries declined to support the action. Although it proposed progressive initiatives about defining cyber norms and capacity development, it failed to address patriotic hackers, cyber militias, or applying the Law of Armed Conflict to the cyber domain.[20] Aside from self-defense against an armed attack, the Security Council is the only means by which offensive action may acquire international legitimacy. NATO has been the UN's enforcement arm in a number of recent actions—

such as ongoing operations against Somali pirates in the Gulf of Aden, and support to Libyan rebels during the overthrow of Moammar Khadafi in 2011. The UN has no permanently assigned armed forces, so NATO's voluntary participation is appreciated and respected by the international community. However, assuming a role as a cyber-security force on behalf of the UN is unlikely until the technology for attribution advances to the point that an attack's origin can be ascertained with precision—and the intrusion's severity is commensurate with an "armed attack." In the meantime, NATO countries experience thousands of intrusive cyber probes every day; the United States alone has its Department of Defense (DoD) networks probed 250,000 times per hour—according to US Cyber Command.[21] The NATO network has about thirty "significant" cyber intrusions every day on its networks, routinely attempting to insert spyware into servers and individual computers.[22] There must be criteria established for a response to cyber events directed against NATO below the unambiguous armed attack level—acceptable under international norms and palatable to members of the alliance.

Under international law, a nation-state is responsible for any unlawful activity emanating from within its borders, provided that it has the capacity to exercise control over the whole of its territory—according to Nicholas Tsagourias, University of Glasgow, an international law and security scholar.[23] From the CCD-CoE's perspective, a member state that suffers a cyber-incident for which another state is responsible may "respond to that violation of international law by resorting to proportionate responses. These may include, where appropriate in the circumstances, countermeasures (Rule 9) or the use of force in self-defence (Rule 13)."[24] Under the *Tallin Manual* 's Rule 9, a NATO nation may employ "proportionate countermeasures, including cyber

countermeasures, against the responsible State," provided that the country does not take actions that constitute use of force, violate fundamental human rights, effect reprisals, or breach the norms of international law.[25] The use of countermeasures would arise when cooperation with an Internet Service Provider is not possible—or outright declined in the nation harboring the non-state cyber actors. Katherine Hinkle defines *countermeasures* as "temporarily lawful actions undertaken by an injured state in response to another state's internationally unlawful conduct."[26] Therefore, a state may take active countermeasures to bring another state into compliance with the law.[27] Countermeasures against centrally controlled botnets may include forcibly redirecting bots to a different server—which instructs bots to uninstall themselves from infected computers.[28] The more sophisticated peer-to-peer bots, which seek other bots but have no central controller, can be infiltrated with fake bots that send code instructing other bots to shut down their own malware.[29] The key word in Hinkle's definition is *state*; the use of countermeasures is more complex with non-state actors. In the case of Estonia, the challenge of attribution presented difficulties in proving that Russia sponsored unlawful cyber activity, but certainly its refusal to stop the DDOS was unlawful. The cyber incident was well-publicized through international media; journalists repeatedly requested comments from Russian officials about the matter—yet the Putin government did nothing to stop it or even investigate the likely locations of the botnet controllers. After days of intermittent DDOS activity, the Estonian General Prosecutor sent a letter to the Russian government—requesting investigation of several suspected cyber militia Internet Protocol (IP) addresses in Russia. The response from his Russian counterpart was dismissive: "We do not co-operate because our criminal code does not recognize

the procedure identification of IP addresses."[30] Ultimately Estonia identified IP addresses associated with botnets in 175 countries. After the incident ended on 19 May, the governments of every nation—except Russia—assisted Estonia in removing the malware that had enslaved unwitting computers.[31] Russia's failure to enforce the rule of law implies tacit permission for cyber militias to operate with impunity; evidence suggests that the untouchable status of Russian patriotic hackers is more by design than lack of law enforcement capacity or expertise.

There are a number of suspicious connections between the Russian government and one of Russia's largest youth groups, calling itself the *Nashi* ("ours")—a pro-Kremlin organization notorious for its association with illicit Internet activity. The *Nashi* were established in 2005, encouraged by Vladislav Surkov—President Putin's first deputy chief of staff. The rapid nature by which *Nashi* mobilized a botnet infrastructure of over one million "zombie" computers suggests the hand of a sophisticated hacker organization cooperating with the cyber militia. In 2007, a Russian cyber-crime organization known as the Russian Business Network (RBN) operated the largest botnets in the world; one of its principle operatives was Aleksandr Boykov—formerly a lieutenant colonel in the *Federalnaya Sluzhba Bezopasnosti* (FSB), the KGB's successor.[32] As a former director of the FSB, President Putin would have been well versed in its covert cyber capabilities, and Boykov's associations with organized crime. RBN's connections with law enforcement through former FSB officers ensured the Russian government's security services never arrested any RBN members; therefore, they were emboldened to rent their "services to cyber criminals and hacker patriots."[33] The FSB had maintained an unsavory relationship with hackers since the early 1990s;

Oleg Gordievsky—a former KGB colonel who defected to British MI6—declared in 1998 that convicted Russian hackers occasionally were offered an alternative to prison: working for the FSB.[34] The London-based Asymmetric Threats Contingency Alliance (ATCA)—comprised of senior international government and private financial sector officials—claimed to have evidence that Moscow "rented time from trans-national criminal syndicates on botnets" and noted that the DDOS ended because "the attackers' time on the rented servers expired, and the botnet attacks fell off abruptly."[35] Perhaps ATCA's analysis was overly circumstantial, but it raises important questions about accountability among nation-states. At the very least, Russia had a responsibility under international law to stop the DDOS being facilitated by botnet controllers located within its geographic borders, and prosecute the cyber criminals involved. "Rule 5" of the *Tallinn Manual* addresses the cyber responsibility of a nation-state: "A State shall not knowingly allow the cyber infrastructure located in its territory…to be used for acts that adversely and unlawfully affect other States."[36] On the surface, it seems obvious that states in collusion with malicious non-state cyber actors may simply claim that they do not meet the *knowingly* test. However, the *Tallinn Manual* also notes that a state is in violation of international law if it "upon notification by another State that [a cyber-disruption] is being carried out, fails to take reasonably feasible measures to terminate the conduct."[37] If the DDOS had terminated within a day or two, Moscow's incognizance would be plausible—but this event was widely reported through international media, and continued for over three weeks.

International law documents suggest that NATO members may come to the aid of one another in cyber matters. The United Nations' *Responsibility of States for*

Internationally Wrongful Acts specifies under Article 48 that states may band together to defend another state "if the obligation breached is owed to a group of States including that State and is established for the protection of a collective interest of the group."[38] This principle of "collective interest" identifies closely with NATO's concept of "collective self-defense"; thus, legal norms should allow NATO countries to act on behalf of one another with cyber countermeasures against non-state actors. NATO has already established a precedent of collective defense against terrorism, and could extend its policy to cyber-terrorism as well. The Center for Strategic & International Studies' (CSIS) James Lewis asserts that cyber-terrorism is "the use of computer network tools to shut down critical national infrastructures (such as energy, transportation, government operations) or to coerce or intimidate a government or civilian population."[39] In the case of Estonia's DDOS in 2007, government operations were virtually shut down for weeks and the populace certainly was intimidated; it is therefore not unreasonable to deem the event "cyber-terrorism" and swing Estonia's NATO allies into cyber action.

Internet anonymity will soon fade into the past; marketing firms are improving their attribution software models massively every year—to the point that advertising is reaching consumers that precisely addresses their respective product interests. Presumably the military cyber professionals among the NATO signatories are developing the same capabilities, albeit in a significantly more advanced fashion. Since nation-states are unlikely to leave their digital fingerprints on malware, the attribution focus comes down to identifying individual IP addresses—frequently disguised through multi-stage attacks that route through a series of unwitting computers, often in different countries.[40] Clever hackers purposely route their Internet traffic through IP addresses

in NATO or well-developed neutral countries; in the United States alone, one in ten computers is infected with botnet malware.[41] This may necessitate standing agreements between member states and their Internet Service Providers (ISPs) to traverse international borders with attribution software, capable of tracing the paths of malware purveyors. IP addresses can be traced to a country of origin over 99% of the time, and to a particular city or region with 90-96% accuracy.[42] Even without discovering the name of a particular non-state actor, NATO would have adequate evidence to approach the country's government in which the offending individual resides, and request that the unlawful breach of sovereignty cease immediately. Failure by the state to act implies international consent for NATO to stop the harmful Internet activity.

Interruptions of commerce that are tantamount to economic blockades are unlawful under the norms of international law unless sanctioned by the UN Security Council and conducted by recognized nation-states. NATO was formed following the Soviet Union's ground blockade of West Berlin in 1948, which caused Western European nations to band together and organize the Berlin Airlift. When Yugoslavian President Slobodan Milošević established a *de facto* economic blockade to intimidate Montenegro in 2000,[43] NATO threatened action that caused its cessation.[44] Estonian Defence Minister Jaak Aaviksoo adamantly declared that the 2007 DDOS "can effectively be compared to when your ports are shut to the sea,"[45] thereby creating a virtual economic blockade. The UN would consider a traditional naval blockade an armed attack. National Research Council Chief Scientist Herbert Lin has endeavored to update the blockade concept for the cyber domain: "In the modern era, the dependence

of a nation's economic relations with the outside world on the Internet may be greater than the dependence of national economies on maritime shipping in the mid-twentieth century."[46] During the *Tallinn Manual*'s drafting the "Group of Experts" carefully considered if a cyber-blockade would equate to a blockade as a matter of law. Their determination was based on the intended effect, which is "to affect negatively the enemy's economy. Since much of present day economic activity is conducted through communications via the Internet…it is reasonable to apply the law of blockade to operations designed to block cyber communications."[47] Living in Europe's "most wired" nation, Estonian citizens were tremendously dependent upon the nation's cyber infrastructure. In 2007 some 60 percent of Estonians used the Internet on a daily basis, and 97 percent of the bank transactions occurred online.[48] This Internet dependence is even greater today, worldwide. The disruptive nature of repeated DDOS events over a three-week period caused banks and government entities to shut off international access to the Internet, thereby isolating Estonia as surely as if its ports were physically blockaded. Businesses were unable to process transactions; the loss of three million euros worth of commerce was not insignificant for a nation with a population the size of Phoenix, Arizona. The United Nations recognizes the employment of blockades as a tool for enforcing sanctions upon a non-compliant nation, but they must be carried out by nation-states and announced prior to taking effect. Establishing a blockade without a UN resolution in place would be unlawful—even more so if it were executed by a non-state actor.

Cyber events rarely occur without some degree of forewarning—perhaps not overtly expressed, but understood by emerging military, political, or diplomatic portents.

Tensions between Russian nationalist sympathizers and native Estonians had been building for weeks before the DDOS events of 2007—which were reflected in the Russian-language youth group Internet chatrooms. In response to concerns about the Bronze Soldier's repositioning, Nikolai Kovalyov—head of the Duma Veteran's Affairs committee and formerly Putin's immediate predecessor as director of the Russian FSB—visited Estonia April 30th 2007 on a "fact finding mission" and demanded the immediate resignation of Estonia's government.[49] Simultaneously, some 600 "analog" members of the *Nashi* blockaded the Estonian Embassy in Moscow and attempted to attack the Estonian ambassador.[50] The Russian government briefly prevented trucks from crossing the border from Estonia near St Petersburg, and declared that repairs to the state railroad system would take place on the links entering Estonia—which effectively shut off oil shipments.[51] Post-event analysis revealed that some of the exact botnets that attacked Estonia had previously been employed just weeks earlier against President Putin's opposition candidate—Garry Kasparov—to prevent him from notifying his followers of the correct opposition rally locations.[52] According to Dennis Bilunov, Kasparov's executive director of the United Civil Front party, "There is a specific department within the FSB…that specializes in coordinating Internet campaigns against those they consider a threat."[53] Estonia's characterization as a "threat" may have resonated strongly with the FSB—particularly since the organization's former boss was Vladimir Putin, appointed by President Boris Yeltsin in 1998. Unlike Yeltsin—who purposely marginalized the FSB's influence on the Kremlin—Putin pulled senior FSB officials into his oligarchical circle of friends from St Petersburg upon taking the presidential reins.[54] On the very day when the DDOS against Estonia reached its

zenith, President Putin delivered a fiery speech in Moscow's Red Square, in which he declared those "who are trying today to desecrate memorials to war heroes are insulting their own people and sowing enmity and new distrust" between the state and its citizens.[55] The Russian parliament even asked President Putin to sever diplomatic relations with Estonia, and initiate an economic blockade.[56] Each of these incidents is an *indicator* in the parlance of intelligence analysts; one can glean an estimate of a group's intent with a reasonable degree of confidence—by assembling the indicators into an overall picture. In describing the events that led up to the DDOS incident, Hillar Aarelaid—director of Estonia's Computer Emergency Response Team (CERT)—opined that "if there are fights on the street, there are going to be fights on the Internet."[57] This assumption has proven correct many times in world events since Estonia's cyber incident in 2007. Georgia incurred a massive DDOS attack during 2008, in conjunction with kinetic attacks by Russia—unsurprisingly using some botnet controller computers associated with the Russian Business Network.[58] The STUXNET cyber weapon appeared after months of international consternation about Iran's nuclear development program in 2011. Understanding potential flashpoints in the physical world provides a clue to what may happen in the cyber domain—which presents an opportunity for predictive intelligence analysis. NATO may be in a position to craft an order similar to the United States' classified "Presidential Directive 20," which purportedly establishes a process to "ensure that U.S. citizens' and foreign allies' data and privacy are protected and international laws of war are followed."[59] According to *Washington Post* reporter Ellen Nakashima in her article "Obama signs secret directive to help thwart cyberattacks," the President has effectively authorized actions that "might include

stopping a computer attack by severing the link between an overseas server and a targeted domestic computer."[60] Taking aggressive anticipatory self-defense measures such as these requires excellent intelligence; fortunately for NATO, intelligence collection is acceptable under the norms of international cyber activity. The United States' National Security Agency collects continuously, as well as the United Kingdom's Government Communications Headquarters (GCHQ); UK members of parliament even opined that GCHQ "look to infiltrate other networks in order to gather intelligence."[61] Canada's Communications Security Establishment has considerable capability, as well as France's cyber warfare specialists in the General Directorate of Armament. Although security classifications may limit the level of detail in threat reporting shared between NATO nations—particularly those that became members after 1991—the use of "tear lines"[62] facilitates information sharing that could detect pending cyber events before they occur. If there were to be another DDOS like the one directed toward Estonia in 2007, the President could now unilaterally sever the links between botnet controllers overseas and the "zombie" computers in the US—as a bilateral action supporting Estonia. NATO signatories carry out bilateral and multilateral activities routinely, as evidenced in the close intelligence cooperation between the US, UK, and Canada. The botnets focused on Estonia had most of their "zombies" established within the US; employing a NATO version of the US "Presidential Directive 20" would sharply reduce the DDOS' effect.

Invoking the *Tallinn Manual*'s Rule 13, using force in self-defense, would only be appropriate if NATO could demonstrate a need for anticipatory self-defense—which is permissible under Article 51 of the UN Charter, provided that it is necessary, discriminatory, and proportional.[63] Article 51 simply states that "[n]othing in the present

Charter shall impair the right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations."[64] By aggregating the norms of Article 48's recognition of collective self-defense and Article 51, one may surmise that it is acceptable for NATO to collectively carry out anticipatory self-defense. However, the UN Charter was originally written with the assumption that anticipatory and collective self-defense would be a matter of states versus states; non-state actors simply were not an issue during the UN Charter's drafting in the years leading up to 1949. The concept of anticipatory self-defense at the time was highly geographic—a state that detected massive forces building upon its border with another state was not compelled to wait for its neighbor to attack before taking countermeasures. The same principles may be applied with anticipatory self-defense when NATO nations detect impending cyber events with international security implications. For example, if NATO discovers that a cyber militia has embedded logic bombs into the air traffic control software at Charles De Gaulle Airport in Paris, and they trace the malware back to servers in Russia, NATO could lawfully launch cyber weapons[65] against the non-state actors if Russia refused to assist in the miscreants' apprehension and prosecution. Logic bombs are capable of halting a computer's operations without warning. Taking action is necessary because of the potentially deadly results of halting the air traffic control system during takeoffs and landings of many aircraft originating in NATO countries. It would be proportional to destroy the cyber militia's capability to reconstitute its logic bomb assault, rather than conduct "kinetic" operations. State Department Senior Legal Advisor Harold Koh made the United States' position very clear on this subject during his address to the USCYBERCOM Inter-Agency Legal Conference in September 2012: "A state's national

right of self-defense, recognized in Article 51 of the UN Charter, may be triggered by computer network activities that amount to an armed attack or imminent threat thereof."[66] Precision may be the most problematic aspect of this defensive act, since IP address spoofing and other techniques by hackers could misdirect NATO's countermeasures against an unwitting host for the malicious attack; advances in attribution technology will likely mitigate this possibility.

Determining which impending cyber threats may have international security implications for the alliance requires deliberation between the respective NATO members' ministers, particularly since some events ultimately will not rise to the level of armed attacks. It is reasonable to assume, though, that countries would seek immediate countermeasures against cyber disruptions that would panic their citizens and reduce confidence in government: outages of critical utilities, transportation disruptions, and shutdowns of critical electronic commerce—such as securities exchanges. As chief scientist of the Computer Science and Telecommunications Board, Herbert Lin believes that "cyber attacks on the controlling information technology for a nation's infrastructure that has a significant impact on the functioning of that infrastructure…would be an armed attack for Article 51 purposes."[67] NATO's most militarily significant members are taking a tougher stance against cyber militias. Secretary of Defense Leon Panetta already suggested the intention to take pre-emptive, aggressive measures in the event of a cyber-disruption directed against the US or its allies, during his remarks in New York City in October 2012.[68] General Keith Alexander—commander of United States Cyber Command—confirmed the new cyber doctrine during congressional testimony in March 2013, with the announcement of

thirteen “defend the nation” offensive cyber teams, capable of stopping pending cyber-attacks.[69] British Members of Parliament published a committee report in July 2012 that suggested a similar approach, specifically targeting non-state actors: “The report recommends the UK employs what it calls ‘active defense: Interfering with the systems of those trying to hack into UK networks’.”[70] British Armed Forces Minister Nick Harvey believes preemptive cyber strikes are a “civilized option” when faced with national security threats; Canadian Defence Minister Peter Gordon Mackay equates an anticipatory cyber strike as an “insurance policy” against aggression.[71] Germany established its Computer Network Operations organization in June 2012—with a mission to conduct offensive cyber operations—in an endeavor to counter Chinese intrusions and more closely mirror the cyber warfare capabilities of the United States, France, and Great Britain.[72] A senior German official purportedly opined—following the DDOS event in Estonia—that NATO’s Article 5 agreement should extend to the cyber domain.[73] The trouble with anticipatory self-defense against non-state actors is in determining intent; some intrusive malware is placed to cause damage—but it is far more common to encounter malware intended for persistent espionage.

International law does not address spying—largely because every country does it and none wants to cease collecting intelligence. Col Gary Brown and Maj Keira Poellet assert in “The Customary International Law of Cyberspace” that since “cyber activities are frequently akin to espionage…most cyber activities can also occur without violating territorial sovereignty.”[74] Applying the “espionage template” to this international legal question suggests that because states recognize spying occurs routinely, they simply cannot do anything about malicious cyber events; the two are presumably too difficult to

distinguish. However, non-state actors like cyber militias or patriotic hackers ostensibly do not have an affiliation with nation-states; therefore, the argument that they may be engaging in digital reconnaissance would not be valid. Only state governments have legitimate intelligence collection requirements and recognized organizations for that purpose. Col Brown observes, too, that cyber espionage has garnered a degree of public condemnation that may distinguish it from physical espionage and its lack of associated interest within international law.[75]

NATO's taking cyber countermeasures is not without its potential problems. Myriam Dunn Cavelty asserts in "Cyber Allies: Strengths and weaknesses of NATO's cyberdefense posture" that attribution of cyber-attacks on member states—linked to Article 5 collective self-defense decisions—is excessively vexatious for the alliance. She anticipates that attribution collection software would be too intrusive on people's privacy, causing an unwelcome increase in regulation for the private sector in all twenty-eight countries. Cavelty believes NATO should focus strictly on cyber-security problems affecting NATO's internal military networks, and address cyber threats to member states through Article 4 procedures—meaning members "will 'consult together' in the case of cyberattacks, but are not duty bound to aid each other as described in Article 5 of the Treaty."[76] In congressional testimony during the July 2010 hearing on "Planning for the Future of Cyber Attack," the Council on Foreign Relations' Robert K. Knake noted that the way in which states respond when confronted with the presence of illicit cyber activity inside their borders indicates their level of commitment to international norms of cyber sovereignty. Furthermore, Knake asserts that states refusing to cooperate in removing cyber threats should expect consequences for their inaction.[77] Therefore, if

NATO were to associate a non-state actor's IP address with the preparation of illicit cyber weapons, it would be permissible as an anticipatory self-defense measure to target the IP address with cyber countermeasures that could prevent the attack's initiation and protect the sovereignty of the NATO signatory involved. There is no requirement under international law that nations must "take the first punch" before responding to threats. This self-defense measure could occur after Article 4 consultations as a bilateral or multi-lateral arrangement between NATO members, or through the Article 5 process. Some NATO nations may have reservations about employing cyber countermeasures under Article 5 procedures, which can be addressed through national caveats. NATO countries have been in Afghanistan for over a decade under an Article 5 collective defense authorization, yet nearly all have national caveats that limit some aspects of their respective forces' operations. German forces were not allowed to patrol at night, and their government limited the *Bundeswehr* to movements by armored vehicles only.[78] Although this caused tension with fellow NATO countries at times, Germany had the right to declare its own force protection measures. The same is true of cyber force protection—individual nations may set their respective rules of cyber engagement, even if NATO invokes Article 5.

Cyber has joined air, land, sea, and space as a fifth operational domain of modern warfare.[79] Since there has not been a thorough overhaul of international law since the highly kinetic 1940s, its application to cyber operations is clumsy and inconsistent. In summary, there are three scenarios in which cyber countermeasures would be appropriate: (1) when a nation-state fails to enforce the rule of law against non-state actors employing cyber disruptions against other states from within its

borders; (2) when a cyber-disruption is tantamount to an economic blockade; and (3) if there is intelligence that indicates a pending cyber-attack by force, thereby necessitating anticipatory self-defense. NATO cannot sit on its collective hands if its members incur another cyber incident on the scale of the DDOS in Estonia during 2007. Since the UN is so hamstrung by procedural issues, NATO must hold nations accountable for failing to address cyber militia activity within their borders. If the harboring nations fail to act, NATO should take measures to cease the illicit activity; there are no other alliances capable of enforcing the international norms of cyber activity. Creating cyber events so severe that they generate an economic blockade is an unlawful use of force, whether the origin is a state or non-state actor. Data from February 2013 published by the *Allianz für Cyber-Sicherheit* (Cyber Security Alliance) determined that—among the top fifteen cyber-attacking countries—the Russian Federation is geographically the IP address location for 32% of the world's cyber-intrusions. Russia and Ukraine combined account for 40% of all cyber-intrusions.[80] China is widely vilified as the most egregious violator of cyber sovereignty, yet the *Allianz* found only 15% of cyber-intrusions originated from China.[81] With the scale of cyber threat emanating from Eastern Europe, NATO must take preemptive countermeasures if it recognizes an imminent cyber-attack against a member state, provided that it is identified by thorough intelligence analysis. Perhaps if Minister of Defence Jaak Aaviksoo could return to May 2007, he would approach his NATO allies with an argument that belatedly occurred to him as the DDOS on Estonia was winding down: "Considering the scale of damage and the way these cyber-attacks have been organised, we can compare them to terrorist activities."[82]

NATO has been fighting terrorism for twelve years; defeating cyber-terrorism by non-state actors is simply an extension of current policy.

Endnotes

[1] Ian Traynor, "Russia accused of unleashing cyberwar to disable Estonia," *The Guardian Online*, May 16, 2007, http://www.guardian.co.uk/world/2007/may/17/topstories3.russia (accessed February 7, 2013)

[2] Kertu Ruus, "Cyber War I: Estonia Attacked from Russia," *European Affairs Online*, vol 9, issue 1-2 (Winter/Spring 2008), linked from *The European Institute Online*, http://www.europeaninstitute.org/2007120267/Winter/Spring-2008/cyber-war-i-estonia-attacked-from-russia.html (accessed January 22, 2013)

[3] Nerijus Adomaitis, "Estonia calm after Red Army site riots, Russia angry," *Reuters Online*, April 28, 2007, http://www.reuters.com/article/2007/04/28/us-estonia-russia-idUSL2873034620070428 (accessed January 22, 2013)

[4] Joshua Davis, "Hackers Take Down the Most Wired Country in Europe," August 21, 2007, *Wired Magazine Online*, Issue 15.09, http://www.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=all (accessed January 22, 2013)

[5] Ibid.

[6] Ibid.

[7] Kara Flook, "Russia and the Cyber Threat," May 13, 2009, *AEI Critical Threats Online*, American Enterprise Institute, http://www.criticalthreats.org/russia/russia-and-cyber-threat (accessed February 7, 2013)

[8] A "packet" is a unit of data routed between an origin and a destination on the Internet. See Margaret Rouse's definition in *SearchNetworking*, http://searchnetworking.techtarget.com/definition/packet (accessed February 12, 2013)

[9] Jason Richards, "Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security," 2009, *International Affairs Review*, http://www.iar-gwu.org/node/65 (accessed February 12, 2013)

[10] Stephen Herzog, "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses," *Journal of Strategic Security Online*, Vol IV (2011), No 2: 53 http://scholarcommons.usf.edu/jss/vol4/iss2/4/ (accessed January 22, 2013)

[11] Toomas Lepik, "Setting the scene: Lessons Learned," February 13, 2008, Estonian Informatics Centre, linked from *Europe's Information Society Thematic Portal:* Workshop on learning from large scale attacks on the Internet – Policy Implications," http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/large_scale/index_en.htm (accessed January 22, 2013)

[12] Calculated with Estonian GDP at $21.279 billion and US GDP of $13.811 trillion. See geohive Global Economy, http://www.geohive.com/charts/ec_gdp1.aspx (accessed February 11, 2013)

[13] Transcribed from Arizona's 2007 Gross State Product (GSP) of $259.2 billion. See US Government Revenue, January 9, 2013, http://www.usgovernmentrevenue.com/compare_state_revenue_2007bZ0a (accessed January 9, 2013)

[14] "Arizona GDP Size and Rank," January 26, 2010, *EconoPost Online*, http://econpost.com/arizonaeconomy/arizona-gdp-size-rank (accessed March 1, 2013)

[15] "The North Atlantic Treaty," April 4, 1949, linked from North Atlantic Treaty Organization Home Page at "e-Library" to "Official Texts," http://www.nato.int/cps/en/natolive/official_texts_17120.htm (accessed December 11, 2012)

[16] George Robertson, "Statement by NATO Secretary General Lord Robertson," October 2, 2001, linked from NATO Speeches, http://www.nato.int/docu/speech/2001/s011002a.htm (accessed February 3, 2013)

[17] Michael N. Schmitt, et al, *The Tallinn Manual On the International Law Applicable to Cyber Warfare Online*: 54, linked from NATO Cooperative Cyber Defence Centre of Excellence at "Publications," http://ccdcoe.org/249.html (accessed February 12, 2013)

[18] "Chapter VII: Action with Respect to Threats to the Peace, Breaches of the Peace, and Acts of Aggression," *Charter of the United Nations Online*, http://www.un.org/en/documents/charter/chapter7.shtml (accessed February 22, 2013)

[19] James R. Clapper, "Unclassified Statement for the Record on the Worldwide Threat Assessment of the US Intelligence Community for the Senate Select Committee on Intelligence," January 31, 2012, www.dni.gov/index.php/newsroom/testimonies (accessed December 11, 2012)

[20] Jason Healey, "Breakthrough or Just Broken? China and Russia's UNGA Proposal on Cyber Norms," *New Atlanticist Online*, September 21, 2012, http://www.acus.org/new_atlanticist/breakthrough-or-just-broken-china-and-russias-unga-proposal-cyber-norms (accessed February 12, 2013)

[21] James G. Stavridis and Elton C Parker, "Sailing the Cyber Sea," *Joint Force Quarterly Online*, vol 65 (April 2012): 63, http://www.ndu.edu/press/sailing-the-cyber-sea.html (accessed December 11, 2012)

[22] Matthias Gebauer, "NATO Faced with Rising Flood of Cyberattacks," *Der Spiegel Online*, April 26, 2012, http://www.spiegel.de/international/world/nato-concerned-about-increasing-numbers-of-cyberattacks-a-829908.html (accessed December 13, 2012)

[23] Nicholas Tsagourias, "Cyber attacks, self-defence, and the problem of attribution," *Journal of Conflict and Security Law*, Vol 17, No 2 (2012): 240, http://jcsl.oxfordjournals.org/content/17/2/229.short (accessed January 18, 2013)

[24] Ibid, 35.

[25] Ibid, 41.

[26] Katherine C. Hinkle, "Countermeasures in the Cyber Context: One More Thing to Worry About," *The Yale Journal of International Law Online*, Vol 37 (Fall 2011): 12, http://www.yjil.org/online/volume-37-fall-2011/countermeasures-in-the-cyber-context-one-more-thing-to-worry-about (accessed January 31, 2013)

[27] Oona Hathaway, "The Law of Cyber-Attack," *California Law Review*, Vol 100 (2012): 857, linked from the Social Science Research Network, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2134932 (accessed March 1, 2013)

[28] Felix Leder, Tillmann Werner, and Peter Martini, "Proactive Botnet Countermeasures: An Offensive Approach," from *The Virtual Battlefield: Perspectives on Cyber Warfare*, 2009, linked from NATO Cooperative Cyber Defence Centre of Excellence 2009 Conference Proceedings, http://www.ccdcoe.org/230.html (accessed March 19, 2013)

[29] Ibid.

[30] Steve Mansfield-Devine, "Estonia: what doesn't kill you makes you stronger," *Network Security*, Vol 2012, Issue 7 (July 2012): 15, www.sciencedirect.com/science/article/pii/S135348581270065X (accessed February 7, 2013)

[31] Ibid, 15.

[32] Kara Flook, "Russia and the Cyber Threat." (accessed February 8, 2013)

[33] Alexander Klimburg, "Mobilising Cyber Power," *Survival: Global Politics and Strategy*, Vol 53, Issue 1 (2011): 49-50 , linked from Taylor & Francis Online, http://www.tandfonline.com/doi/abs/10.1080/00396338.2011.555595 (accessed January 24, 2013)

[34] Kara Flook, "Russia and the Cyber Threat." (accessed February 8, 2013)

[35] Iain Thomson, "Russia 'hired botnets' for Estonia cyber war," May 31, 2007, *V3.co.uk*, http://www.v3.co.uk/v3-uk/news/1974750/russia-hired-botnets-estonia-cyber-war (accessed January 24, 2013)

[36] Michael N. Schmitt, *Tallinn Manual*, 33.

[37] Ibid, 34.

[38] International Law Commission, "Responsibility of States for Internationally wrongful acts," 2001, www.ilsa.org/jessup/jessup06/basicmats2/DASR.pdf (accessed January 18, 2013)

[39] James A. Lewis, "Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats," December 2002: 1, Center for Strategic & International Studies, http://csis.org/files/media/csis/pubs/021101_risks_of_cyberterror.pdf (accessed February 22, 2013)

[40] David D. Clark and Susan Landau, "Untangling Attribution," *Harvard National Security Journal*, vol 2, issue 2 (2011): 334, in HeinOnline (accessed December 12, 2012)

[41] Grant Gross, "White House Launches Coordinated Effort to Battle Botnets," May 30, 2012, *PCWorld Online*, http://www.pcworld.com/article/256507/white_house_launches_coordinated_effort_to_battle_botnets.html (accessed March 1, 2013)

[42] David D. Clark and Susan Landau, "Untangling Attribution," 340.

[43] Carlotta Gall, "Montenegrin Says Belgrade Is Using Its Army to Oust Him," *The New York Times Online*, March 28, 2000, http://www.nytimes.com/2000/03/28/world/montenegrin-says-belgrade-is-using-its-army-to-oust-him.html (accessed March 18, 2013)

[44] "Robertson warns Milosevic on Montenegro," *NATO Newspages Online*, September 27, 2000, http://www.nato.int/docu/newspage/2000/n000927e.htm (accessed March 18, 2013)

[45] Mark Landler and John Markoff, "Digital Fears Emerge After Data Siege in Estonia," May 29, 2007, *The New York Times Online*, http://www.nytimes.com/2007/05/29/technology/29estonia.html?pagewanted=all&_r=0 (accessed February 22, 2013)

[46] Herbert S. Lin, "Offensive Cyber Operations and the Use of Force," *Journal of National Security Law & Policy Online*, Vol 4, No 63 (2010): 81, from HeinOnline, http://heinonline.org/HOL/Page?handle=hein.journals/jnatselp4&div=9&g_sent=1&collection=journals (accessed February 22, 2013)

[47] Michael N. Schmitt, *Tallinn Manual*, 162.

[48] Stephen Herzog, "Revisiting the Estonian Cyber Attacks," 51.

[49] Victor Yasmann, "Russia: Monument Dispute with Estonia Gets Dirty," May 4, 2007, *Radio Free Europe: Radio Liberty Online*, http://www.rferl.org/content/article/1076297.html (accessed February 8, 2013)

[50] René Värk, "The Siege of the Estonian Embassy in Moscow: Protection of a Diplomatic Mission and Its Staff in the Receiving State," *Juridica International Online*, Vol XV (2008), http://www.juridicainternational.eu/index.php?id=12739 (accessed February 8, 2013)

[51] Steven Lee Myers, Tensions Worsen Between Russia and Estonia," *The New York Times Online*, May 2, 2007, http://www.nytimes.com/2007/05/02/world/europe/02iht-estonia.4.5537016.html?_r=0 (accessed February 11, 2013)

[52] Joshua Davis, "Hackers Take Down the Most Wired Country in Europe," (accessed February 11, 2013)

[53] Ibid.

[54] "The making of a neo-KGB state: Political power in Russia now lies with the FSB, the KGB's successor," August 23, 2007, *The Economist Online*, http://www.economist.com/node/9682621 (accessed February 18, 2013)

[55] Adrian Blomfield, "Putin criticizes Estonia over war memorial," May 10, 2007, *The Telegraph Online*, http://www.telegraph.co.uk/news/worldnews/1551174/Putin-criticises-Estonia-over-war-memorial.html (accessed February 12, 2013)

[56] Ibid.

[57] Mark Landler and John Markoff, "Digital Fears Emerge After Data Siege in Estonia."

[58] John Markoff, "Before the Gunfire, Cyberattacks," *The New York Times Online*, August 12, 2008, http://www.nytimes.com/2008/08/13/technology/13cyber.html?_r=0 (accessed March 17, 2013)

[59] Ellen Nakashima, "Obama signs secret directive to help thwart cyberattacks," *Washington Post Online*, November 14, 2012, http://articles.washingtonpost.com/2012-11-14/world/35505871_1_networks-cyberattacks-defense (accessed December 13, 2012)

[60] Ibid.

[61] Steve Evans, "UK should strike first in cyber war, MPs say," *Computer Business Review*, linked from "Security News," July 18, 2012, http://security.cbronline.com/news/uk-should-strike-first-in-cyber-war-mps-say-180712 (accessed March 17, 2013)

[62] "Tear lines" are simply "watered down" intelligence. They convey threats in general terms without specifying the sources and methods employed to collect the intelligence.

[63] Stephen Dycus, et al, Aspen Casebook Series, *National Security Law*, 5th ed. (New York: Wolters Kluwer Law & Business, 2011), 350.

[64] United Nations, "Charter of the United Nations," December 10, 2012, linked from *United Nations Homepage* at "Documents," http://www.un.org/en/documents/charter/chapter7.shtml (accessed December 17, 2012)

[65] A "cyber weapon" is defined as any "cyber device, materiel, instrument, mechanism, equipment, or software used, designed, or intended to be used to conduct a cyber-attack. See Michael N. Schmitt's "International Law in Cyberspace: The Koh Speech and Tallinn Manual juxtaposed," *Harvard International Law Journal*, vol 54 (December 2012), http://www.harvardilj.org (accessed December 18, 2012)

[66] Harold Hongju Koh, "International Law in Cyberspace," linked from *Harvard International Law Journal Online*, vol 54 (December 2012), http://www.harvardilj.org/ (accessed December 18, 2012)

[67] Herbert S. Lin, "Offensive Cyber Operations and the Use of Force," 74.

[68] Phil Stewart, "U.S. defense chief says pre-emptive action possible over cyber threat," *Reuters Online*, October 11, 2012, linked from "Top News,"

http://mobile.reuters.com/article/idUSBRE89B04Q20121012?irpc=932 (accessed December 14, 2012)

[69] Richard Lardner, "Pentagon forming cyber teams to prevent attacks," *Washington Times Online*, March 12, 2013, http://www.washingtontimes.com/news/2013/mar/12/pentagon-forming-cyber-teams-to-prevent-attacks/?page=all (accessed March 18, 2013)

[70] Steve Evans, "UK should strike first in cyber war, MPs say."

[71] Agence France Press, "Cyber strikes a 'civilized' option: Britain," *Inquirer Technology*, June 3, 2012, linked from "Headlines," http://technology.inquirer.net/11747/cyber-strikes-a-civilized-option-britain (accessed December 17, 2012)

[72] Jorge Benitez, "Germany reveals offensive cyberwarfare capability," *NATO Source*, June, 8, 2012, linked from The Atlantic Council, http://www.acus.org/natosource/germany-reveals-offensive-cyberwarfare-capability (accessed December 17, 2012)

[73] James A. Lewis, "The 'Korean' Cyber Attacks and their Implications for Cyber Conflict," October 2009: 3, Center for Strategic & International Studies, http://csis.org/files/publication/091023_Korean_Cyber_Attacks_and_Their_Implications_for_Cyber_Conflict.pdf (accessed February 22, 2013)

[74] Gary Brown and Keira Poellet, "The Customary International Law of Cyberspace," *Strategic Studies Quarterly*, Fall 2012: 134, www.au.af.mil/au/ssq/2012/fall/brown-poellet.pdf (accessed February 18, 2013)

[75] J. Nicholas Hoover, "Cyber Warfare Still Poses Legal Questions," *InformationWeek Government Online*, September 19, 2012, http://www.informationweek.com/government/security/cyber-warfare-still-poses-legal-question/240007560 (accessed March 17, 2013)

[76] Myriam Dunn Cavelty, "Cyber Allies: Strengths and weaknesses of NATO's cyberdefense posture," *Internationale Politik*, vol 12/3 (February 1, 2012): 13, in Social Science Research Network (accessed December 12, 2012)

[77] Robert K. Knake, "Untangling Attribution: Moving to Accountability in Cyberspace," from the Congressional *Hearing on Planning for the Future of Cyber Attack*, July 15, 2010, in "Publications," under "Testimony," http://www.cfr.org/united-states/untangling-attribution-moving-accountability-cyberspace/p22630 (accessed December 12, 2012)

[78] John Nagl and Richard Weitz, "Counterinsurgency and the Future of NATO," *Chicago Council Transatlantic Paper Series No 1*, October 2010: 11, http://www.cnas.org/node/5337 (accessed March 17, 2013)

[79] Mark Clayton, "Pentagon unveils its new cyberstrategy. Well, some of it, anyway," *The Christian Science Monitor Online*, July 14, 2011, http://www.csmonitor.com/USA/Military/2011/0714/Pentagon-unveils-its-new-cyberstrategy.-Well-some-of-it-anyway (accessed February 18, 2013)

[80] In February 2013 Deutsche Telekom and the *Allianz für Cyber-Sicherheit* detected 7,407,348 cyber-attacks from the top 15 source nations. Russia accounted for 2,402,722 and Ukraine originated 566,531. See Allianz für Cyber-Sicherheit's "Overview of current cyber attacks (logged by 97 sensors), http://www.sicherheitstacho.eu/?lang=de (accessed March 19, 2013)

[81] Ibid. The *Allianz* reported 1,075,248 intrusions between Taiwan Province and China.

[82] "Estonia urges firm EU, NATO response to new form of warfare: cyber-attacks," *The Sydney Morning Herald* Online, May 16, 2007, http://www.smh.com.au/news/Technology/Estonia-urges-firm-EU-NATO-response-to-new-form-of-warfarecyberattacks/2007/05/16/1178995207414.html (accessed February 18, 2013)